DECLARATION OF PATRICK PAIGE

I, PATRICK PAIGE, DO HEREBY DECLARE:

1. I am over the age of eighteen (18) and otherwise competent to make this declaration. The facts stated in this declaration are based upon my personal knowledge.

2. I was a police officer from 1989 until 2011 for the Palm Beach County Sherriff's Department. And, from 2000-2011, I was a detective in the computer crimes unit.

3. As a detective in the computer crimes unit, I investigated internet child pornography and computer crime cases.

4. I have conducted forensic computer examinations for:

(a) Broward County Sheriff's Office (BSO);

(b) Federal Bureau of Investigation (FBI);

(c) U.S. Customs and Border Protection (CBP);

(d) Florida Department of Law Enforcement (FDLE);

(e) U.S. Secret Service;

(f) Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF); and

(g) Various municipalities in the jurisdiction of Palm Beach County.

5. I was also previously assigned to a police unit working in conjunction with TLO Corp., which is a private company.

6. When I worked with TLO Corp., I supervised the other detectives assigned to the unit, which was consisted of six online investigators and two computer forensic examiners.

7. I am familiar with software programs used to investigate computers, including EnCase and Access Data.

EXHIBIT B

8. I have taken over 400 hours of courses designed to teach people how to investigate computers.

9. Also, while working from 2003-2011 for Guidance Software, the makers of EnCase, I have taught over 375 hours of courses in computer forensics ranging from beginner to advanced levels.

10. I have had students in my courses from various government branches, including: (a) sheriff's offices; (b) FBI agents; (c) ATF agents; (d) agents from the Central Intelligence Agency, and (e) individuals from other branches of government and the private sector.

11. After leaving the Palm Beach County Sherriff's office, I founded Computer Forensics, LLC, where I am currently employed.

12. I have received the following awards and commendations:

(a) 1991 – Deputy of the Year, awarded by the 100 Men's Club of Boca Raton & Rotary Club.

(b) 1997 – Deputy of the Month for June.

(c) 2001 – Detective of the Month for October.

(d) 2002 – Outstanding Law Enforcement Officer of the Year, awarded by the United States Justice Department for work in the *U.S. vs. Jerrold Levy* case.

(e) 2003 – U.S. Customs Service Unit Commendation Citation Award for computer forensic work in Operation Hamlet. Operation Hamlet was one of the largest rings in the history of U.S. Customs of individuals who were molesting their own children, and transmitting the images and video via the Internet.

(f) 2005 – Detective of the Month for December.

(g) 2007 – Outstanding Law Enforcement Officer of the Year, awarded by the United States Justice Department for work in the *U.S. vs. Jimmy Oliver* case.

(h) 2008 – Letter of Commendation issued by the FBI for outstanding computer forensic work in the *U.S. vs. Frank Grasso* case.

13. I have been called to testify as a fact and expert witness on numerous occasions in the field of computer forensics in both trial-level and appellate proceedings before state, federal, and military courts in Florida, California, New Jersey, and New York.

14. No court has ever refused to accept my testimony on the basis that I was not an expert in computer forensics. My skill set and my reputation are my most important assets in my current position with Computer Forensics, LLC.

15. With regard to my experience investigating child pornography cases, I supervised police officers whose responsibility it was to establish a successful TCP/IP connection with persons who were sending pornographic images of children or other illegal content over the Internet.

16. The offenders' IP addresses, as well as the dates and times of the illegal transmission were recorded.

17. An officer would then request that the assistant state attorney subpoena the corresponding ISPs for the purpose of identifying the subscribers that were transmitting the illegal content.

18. In these cases, the subscribers were not notified by the ISPs that their identity was being subpoenaed because they could have deleted the images and destroyed the data.

19. After receiving the subscribers' identities, we would prepare a search warrant that would authorize us to enter the subscribers' dwelling and seize all of their computer devices.

20. I was directly involved in approximately 200 search warrants either by way of managing the process or performing it personally.

21. I can recall only one instance in all the times that we executed a search warrant and seized computers where we did not find the illegal content at the dwelling identified in the search warrant.

22. In that one instance, the Wi-Fi connection was not password protected, and the offender was a neighbor behind the residence.

23. I never came across a Wi-Fi hacker situation.

24. In my opinion, a child pornographer has a greater incentive to hack someone's Wi-Fi connection than a BitTorrent user because transmission of child pornography is a very serious crime with heavy criminal penalties, and many offenders can face life sentences if convicted.

25. I tested IPP International U.G.'s ("IPP") IP detection process.

26. To do so, I downloaded four public domain movies from the national archive.

27. I then encoded text into the videos, so that I would know whether someone that downloaded that particular movie downloaded the version of the movie that I created.

28. I then rented four virtual servers, each of which was connected to the Internet and used a unique IP addresses.

29. I then configured the servers so that all of them were running Windows 2008 server edition, and I put a different BitTorrent client onto each server.

30. A BitTorrent "client" is software that enables the BitTorrent protocol to work.

31. After installing the BitTorrent clients, I also installed Wireshark onto each server. "Wireshark" is a program that captures network traffic and creates PCAPs, just as TCP Dump, which IPP uses, does. A PCAP is like a video recording of all the incoming and outgoing transactions of a computer.

32. After installing Wireshark onto each of the servers, I transferred the movies from my local computer to the servers.

33. I then used the BitTorrent clients on each of the servers to make .torrent files. I uploaded these .torrent files onto various torrent websites.

34. I then informed IPP of the movie names. Thereafter, IPP sent me screen captures of the movies I had seeded.

35. The screen captures sent by IPP had my codes on them; thus, I knew that IPP had caught the movies I had seeded.

36. IPP also sent me additional data identifying the IP Address used by each of the four servers, and sent me PCAPs.

37. I reviewed IPP's PCAPs vis-à-vis the PCAP log files created by each of my test servers, and determined that IPP's PCAPs match my PCAPs. This could not have happened unless IPP's server was connected to the test server because the transactions would not match.

38. From this test, I concluded that IPP's software worked, and had a subpoena been issued for my IP addresses, it would have revealed my identity.

FURTHER DECLARANT SAYETH NAUGHT.

DECLARATION

PURSUANT TO 28 U.S.C. § 1746, I hereby declare under penalty of perjury that the foregoing is true and correct.

Executed on this 14th day of March, 2014.

By:________________________
PATRICK PAIGE